DEPARTMENT OF FINANCE BILL ANALYSIS

AMENDMENT DATE: March 4, 2009
POSITION: Neutral

BILL NUMBER: SB 20
AUTHOR: J. Simitian
RELATED BILLS: None

BILL SUMMARY: Personal Information: Privacy

This bill amends current security breach notification law as specified in Sections 1798.29 and 1798.82 of the Civil Code. These sections apply to state agencies, persons or businesses conducting business in California that own or license computerized data that includes personal information. The bill has three components:

1. Specify security breach notices be written in plain language and include certain standard information.
2. Require the Attorney General (AG) be notified if more than 500 California residents are affected by a single breach.
3. Require the Office of Information Security and Privacy Protection (OISPP) be notified if the substitute notice provision in current law is used as notification.

Specified Content for Security Breach Notifications
In addition to being written in plain language, the bill would also require that breach notifications include the following:

- Reporting agency contact information
- Type of personal information believed to have been breached
- Date or date range of occurrence, if possible to ascertain, and the date of the notice
- Whether notification was delayed due to a law enforcement investigation
- General description of breach incident
- Estimated number of persons affected by the breach
- Credit agency contact information if breach involves certain types of information

The bill also suggests that, at its discretion, the agency may include information about what the agency has done in response to the breach and advice on steps victims of a breach may take to protect themselves.

Notification to the Attorney General
The bill requires that if more than 500 California residents are affected by a single breach, electronic notification must be provided to the AG.

Notification to the OISPP
The bill requires that if the substitute notice provision in current law is used, OISPP must also be notified. (Substitute notice consists of all of the following: e-mailing the notification to affected persons if their e-mail address is available; posting the notification on the person, business, or agency's website, if there is one; and notifying major statewide media. Substitute notice is permitted if the cost of providing notice would exceed $250,000, the number of persons affected by the breach exceeds 500,000, or if the agency does not have sufficient contact information.)

Analyst/Principal (0843) R. Gillihan	Date	Program Budget Manager Diana Ducay	Date
Department Deputy Director			Date
Governor's Office:	By:	Date:	Position Approved_____ Position Disapproved_____

FISCAL SUMMARY

Specified Content for Security Breach Notifications
There may be additional staff resources necessary to collect the information required for the breach notification. The extent of the additional amount of staff resources is unknown. Finance contacted the Department of Health Care Services (DHCS) as a representative department that, given the size of the population they serve, would have to provide notification to large numbers of people in the event of a security breach. DHCS indicated that their notification already includes all of the standard content specified in the bill and as a state agency they are already required to notify OISPP. Their only concern was the requirement to notify the AG if more than 500 persons were impacted by the breach. DHCS pointed out that the severity of the breach should determine whether the AG is notified and, by using a set number, it is inconsistent with the security incident reporting requirements of the OISPP, which are based on the nature of the incident, not the number of people impacted.

Notification to the Attorney General
There may be additional staff resources necessary to receive the notifications and handle them, possibly through logging them in and posting them to a website. The AG indicates this could be accomplished with existing staff resources.

Notification to the OISPP
OISPP has indicated that this bill would have minimal fiscal impact on their agency. Existing policy in Section 5350.1 of the State Administrative Manual already requires state agencies to report security breaches to OISPP.

COMMENTS

Primarily due to the limited fiscal impact to the state, Finance is neutral regarding the three components of this bill: specified content for security breach notifications, notification to the AG, and notification to the OISPP. However, certain stakeholders and interested parties have expressed support, opposition, or concerns with the content of the bill as noted below:

- Support: The Privacy Rights Clearinghouse, a consumer advocacy group dedicated to protecting consumers against identity theft and other types of privacy crime, supports this bill. They articulated their support in a letter to Senator Simitian's office dated March 18, 2009.
- Concerned: The California Credit Union League is not opposed to the bill, but has some concerns regarding whether some of the specified content would be known at the time the notice is provided. They are in conversation with the author to possibly amend the language of the bill to provide that specified items of information must be included in the security breach notification, if available at the time the notice is provided.
- Opposed: A number of groups, including the State Privacy and Security Coalition that counts Google, Yahoo, and AOL as members, are opposed to the bill as they feel that current breach notification requirements are sufficient. They are concerned that providing the date of a breach gives a hacker an opportunity to determine whether his or her attack was successful. They are also concerned that providing customers with credit agency contact information implies that all breaches result in fraud and identity theft. They expressed these concerns in a letter to the Senate Judiciary Committee dated February 12, 2009.

Specified Content for Security Breach Notifications

- Fiscal impact to state agencies is most likely extremely minor, if any. According to the author's staff, the bill is mainly directed at the private sector.
- Breach notifications provided by state agencies, in at least one case, already include the content specified in this bill.

Notification to the Attorney General

The AG does not take a position on this bill, however staff commented that most likely an e-mail address would be established to receive the notifications, which would then be posted to the AG website. Staff further commented that as statistical tracking of breaches is already performed by OISPP, it is not clear the further benefit of notifying the AG as well. Staff added that the California Highway Patrol receives breach information from state agencies, but not from the private sector.

OISPP notes that notifying the AG makes the breach a matter of public record, giving the industry access to this information which could assist policymakers by providing them with more information on the scope and nature of security breaches.

Notification to the OISPP

- Fiscal impact to state agencies is most likely extremely minor, if any, as they are already required to report security incidents to the OISPP, regardless of whether they resulted in a breach notification.
- Fiscal impact to OISPP as a result of receiving security breach notifications from persons or businesses is unknown, but most likely minor.

General Comments

We note that, as persons and businesses are currently subject to breach notification requirements, the fiscal/non-fiscal impact of this bill on these entities would likely be minimal.

We also note that Governor's Reorganization Plan No. 1 (Information Technology) proposes to eliminate the OISPP, and instead create the Office of Information Security within the Office of the State Chief Information Officer, and the Office of Privacy Protection within the State and Consumer Services Agency. Because of this potential split in responsibilities, it is unknown which entity would be the recipient of breach notifications.

	SO	(Fiscal Impact by Fiscal Year)						
Code/Department	LA	(Dollars in Thousands)						
Agency or Revenue	CO	PROP						Fund
Type	RV	98	FC	2008-2009	FC	2009-2010	FC	2010-2011	Code
0820/Justice	SO	No		---------- No/Minor Fiscal Impact ----------					0001
0510/Secty SCS	SO	No		---------- No/Minor Fiscal Impact ----------					0001